Which?, 2 Marylebone Road, London, NW1 4DF
Date: 30 June 2017
Response by: Which?

APP scams project team
Payment Systems Regulator
25 The North Colonnade
Canary Wharf
London
E14 5HS

About Which?

Which? is the largest independent consumer organisation in the UK with more than 1.5 million members and supporters. Our mission is to make individuals as powerful as the organisations in their daily lives. We tackle consumer detriment through the products and services we offer and through our campaigns to drive change. We are an a-political, independent social enterprise working for all consumers and funded solely by our commercial ventures. We receive no government money, public donations, or other fundraising income.

Summary

- The PSR should bring forward a package of measures to improve the monitoring and reporting of suspicious patterns of transactions, in order to reduce instances of push payment fraud. PSOs should play a central role, both in acting as the central monitoring point of payment transactions, and in enabling communication about fraud between PSPs.

- The PSR should further explore the introduction of a chargeback scheme to refund consumers who are victims of push payment fraud. This would ensure that the consumer is not left out of pocket and undo the financial harm from most types of push payment fraud. The introduction of a chargeback scheme could also act as an incentive for industry to do more to prevent the fraud from happening in the first place, ultimately reducing the amount they needed to refund.

- The PSR should bring forward the introduction of Confirmation of Payee for authorised push payments. This would let the consumer check that they were transferring funds to the correct payee, before they made a payment. Where the correct payee could not be confirmed, the consumer would be able to stop any loss of funds and alert the authorities to the potential fraud before it has happened.

- Whatever measures the regulator decides to take, they should meet three criteria:
    - Taken together, the measures should address all types of APP fraud.
    - The measures should be based on a thorough analysis of the costs and benefit to consumers.
    - The PSR should monitor the measures against the goal of reducing consumer harm. If they fall short of this goal, then the PSR should amend the measures.

Introduction

Which? welcomes the opportunity to comment on the Payment Systems Regulator's consultation on the role of payment system operators (PSOs) in protecting consumers from falling victim to authorised push payment (APP) scams, and from limiting harm to those who do. Our super-complaint identified that there was significant consumer detriment from this type of fraud, and we support strong action to address the consumer harm.

Push payment fraud remains a significant consumer issue and there needs to be more action from the payments industry to prevent consumers losing life-changing amounts of money. In the six months since the PSR responded to our super complaint, Which? has continued to receive reports of consumers being tricked into making a payment to a fraudster. Our recent research[1] found that of those people who had lost money to bank transfer scams, more than half (54%) had been victims in the last six months. The PSR has acknowledged that the prevalence of APP scams is likely to increase, which clearly demonstrates the need for swift, effective action in this area.

We recognise that Financial Fraud Action UK (FFA UK) is undertaking a separate piece of work to understand any barriers to data-sharing and develop best practice in responding to fraud, as well as in collecting data on the incidence of these types of scams. However, the industry's focus so far has been to promote awareness campaigns focused at educating consumers. We have yet to see evidence that initiatives like the industry backed 'Take Five' campaign have had a significant impact on reducing consumer detriment from APP fraud. In FFA UK's annual review for 2017[2] it acknowledges that: "Changing behaviour does not happen overnight, but so far 65% of those who have seen the campaign say they would behave differently the next time they face a potentially risky scenario". Meanwhile, consumers continue to lose money, and in this particular type of scam, the consumer is not always best placed to identify whether they are in a risky scenario and so be able to take the action that they may otherwise take to enable them to avoid falling victim to the fraud.

Therefore, Which? supports the move by the PSR to identify where other organisations active in the authorised push payments market, such as PSOs, can play a greater role in identifying and tackling fraudulent behaviour. However, whatever measures the regulator decides to take, they should meet the following criteria.

Firstly, the package of measures, as a whole, must address all types of APP fraud – including both malicious misdirection and malicious payee fraud. Solutions that only tackle some types of push payment scams would not lead to a lasting reduction in this type of fraud. As rules change to catch up with fraudsters' current techniques, the fraudster is likely to have already adapted their approach and will turn their attention to any remaining weaknesses or gaps in the system.

Secondly, it should be clear that any measures are based on a thorough analysis of the costs and benefits to consumers - not simply the ease with which they can be implemented. The regulator must assess any measures, based on testing, against the costs and benefits to the consumer. Only then can it identify the precise measures that PSOs should either take

[1] Populus, on behalf on Which? spoke to 2,117 nationally representative UK adults via an online poll between the 3rd and 4th May 2017.

[2] Financial Fraud Action UK, Annual Review 2017, June 2017

themselves or require the payment system providers to take as part of any agreement to use their system.

Finally, it is crucial that, once introduced, the measures are monitored to understand how successful they are at delivering the outcome of reduced consumer harm, and if they fall short of this goal, then the PSR should amend the measures. A core part of the rationale behind Which?'s original intervention on this issue was to ensure that, by whichever means most appropriate, consumers would be far less likely to suffer detriment from falling victim to an authorised push payment scam. Therefore, whether the PSR's proposals are successful or not can only be judged on any reduction in consumers losing money via this type of fraud. If this does not happen, the PSR must consider alternatives to protect consumers from this detriment.

The role of PSOs in helping to reduce consumer harm from APP scams

The PSR suggests a role for PSOs in centrally monitoring payments, and introducing a way for PSPs and PSOs to alert one another when they identify suspicious transactions. Which? agrees that one of the most crucial roles that PSOs can play in helping to tackle authorised push payment fraud is in the monitoring and reporting of suspicious transactions, and in the development of fraud-related communication through the central system infrastructure.

PSOs are key to the process of facilitating the transactions between banks, and in that role they are able to have a more complete overview of the scale and pattern of fraudulent payments than any individual bank, which could only see those that relate to an account it holds. A package of measures to improve the on-going monitoring, detection, and reporting of suspicious patterns of transactions, when combined, should make it more difficult for fraudsters to operate.

<u>The centralised monitoring of payment transactions</u>
A PSO is the only actor in the payment system that could have oversight of every payment made using its system, which puts PSOs in a far stronger position than individual payment service providers (PSPs) - such as banks - to identify system-wide suspicious patterns of transactions that may be invisible to any one bank.

Suspicious patterns of transactions should be understood first and the understanding updated using transactional data from accounts known to have been used for fraudulent purposes. The sorts of patterns this might identify could include where payments of large sums are being transferred over a short period of time from a number accounts held in multiple different banks into one account, particularly where the receiving account was newly established or where the funds were being immediately transferred out again. Whilst each individual bank may be able to see part of the picture, the PSO would have a greater overview and the ability to identify any suspicious trends more quickly, given its access to more data.

This would also give them the intelligence to identify larger system-wide changes to understanding 'suspicious patterns' as fraudsters' practices evolve. Currently each bank has their own individual systems and processes for monitoring suspicious patterns of payments. However, no matter how good these systems are they will only have information on payments that are linked to accounts held by their bank, and therefore on their own can only ever see part of the picture. Enabling and requiring PSOs to play a greater role means that they can

provide a consistent definition of suspicious patterns across banks, adding to the data that is already available to those banks from their own monitoring activity.

Enabling fraud-related communication

Not only can PSOs play a greater role in centrally monitoring payments, they can also facilitate communication between PSPs and PSOs to alert each other when they identify suspicious transactions. Which? agrees that the development of fraud-related communication through the central system infrastructure would be valuable in helping the industry as a whole tackle APP scams. As the regulator notes, such a system could enable the central system and/or sending PSPs to flag potentially fraudulent payments to receiving PSPs.

One of the problems in tackling APP fraud that we have previously highlighted is to overcome the difference in incentives, and ability to act, faced by sending and receiving banks for a given instance of fraud. Moving to a more centralised system could overcome this issue and therefore enable swifter, co-ordinated action across the industry when a potentially fraudulent account is identified.

If the regulator implements these type of measures, it could expect to be in a position where PSPs and PSOs are better equipped to prevent APP fraud before it is committed - the best way to prevent consumer harm. These measures could also tackle all types of fraud and crucially would be future-proofed as they could evolve as fraudsters' practices evolve by amending the definition of 'suspicious transactions' as more fraudulent accounts are identified.

As Which? has previously stated, too much of the current focus for tackling push payment fraud relies on educating consumers so that they are aware and can spot that a fraud is being committed. Where that fails, consumers are encouraged to report the case once they have discovered the fraud. This puts too much emphasis on the consumer, who is often not best placed to make a judgement in identifying the fraud, particularly as these types of scams are becoming increasingly sophisticated. An approach that focuses on the identification by PSOs of accounts that may be being used for fraud may be more effective than relying on consumers to identify and report an instance of fraud.

Which? does not believe that these types of measures would be entirely new to banks; rather they would build on banks' existing work in monitoring suspicious transactions.

We therefore support the PSR's suggestion that PSOs could act as a central monitor of payments, and facilitate communication between banks, which can help to prevent further fraud and identify other potential victims who have paid money to a fraudulent account

The role of a "chargeback" type mechanism, similar to that in place for card-based pull payment systems, for consumer-initiated push payments

As the PSR notes, 'chargeback' is a mechanism which is already used for other payment methods. Other forms of payment, such as debit or credit card, allow the consumer to reclaim money through chargeback in particular cases, for example when goods or services are not provided, or where they are different to the description. Which? believes there is merit in considering how introducing a similar scheme for authorised push payments would help reduce consumer harm, including from fraudulent activity. If push payments are to become a more common way of paying businesses under Open Banking, a chargeback scheme could mirror the

rights that consumers already have when using a credit or debit card. Introducing a chargeback scheme would ensure that the consumer is not left out of pocket and undo the financial harm from most types of push payment fraud.

In addition to reducing financial harm, a chargeback scheme could also contribute to the on-going understand of the evolving patterns of fraud, by providing an additional reporting method of fraudulent accounts to those proactively identified by banks and the PSO. If this additional evidence gathering is successful, we would expect it to lead to a reduction in the number of cases where consumers transfer money to fraudsters, which in turn would mean that less people would require the use of a chargeback scheme.

We understand that there are concerns that a chargeback scheme would itself become a vehicle for fraudulent activity. However, we feel this could be mitigated through careful design by the regulator (such as rules around the standard of proof required to process a chargeback), whilst still ensuring that it would offer a meaningful way for consumers to reclaim money that had been lost to a fraudster. This should form part of the regulator's cost-benefit analysis for any proposed scheme. This analysis should also explore how such a scheme could operate for payments made to personal accounts – unlike existing chargeback mechanisms for card payments, which require a merchant account to receive the payment.

Introducing a chargeback scheme could also act as an incentive for all banks to do more to prevent fraud from taking place in the first place, therefore mitigating the need to rely on a chargeback scheme. There could be a commercial advantage for banks who come up to the level of 'best in class' for fraud prevention, for if banks that have not followed certain 'best practice' procedures, a consumer would be successful in a chargeback claim. The regulator and PSOs should consider how a chargeback scheme's operation could incentivise banks to meet a high standard of fraud prevention.

An alternative method of ensuring that a consumer who has transferred money to a fraudulent account does not suffer financial harm would be for the industry to create an insurance scheme amongst the banks. This could be funded in a variety of ways and Which? would expect the regulator to explore this possibility, and test any proposals to ensure that it did not create a barrier to consumers using push payments to transfer funds.

The role of 'Confirmation of Payee' in reducing consumer detriment from authorised push payments

There are a number of measures that have already been proposed by the regulator as part of the New Payments Architecture, in particular, 'Confirmation of Payee' which is due to be implemented by 2020.

Which? supports the introduction of a measure that would enable the verification of the payee, which would allow consumers to have confidence that the account they are transferring money into belongs to the individual or business they intend to pay.

Whilst this measure alone would not tackle all types of authorised push payment fraud, it would help in incidences where the fraudster had been able to fool the payee that they were an existing trusted or legitimate contact (such as a solicitor, or a construction company), and attempts to maliciously misdirect a payment into the fraudster's own account. In addition, it

would help reduce other misdirected payments that are caused by errors rather than criminal behaviour.

Although the regulator has proposed that this will be introduced by 2020, any steps to introduce this more swiftly could have a significant impact in reducing the overall number of incidences of push payment scams and prevent consumers from losing life-changing sums of money. Which? urges the PSR to ensure that Confirmation of Payee is introduced as soon as possible, and at the very least the regulator must ensure that the 2020 deadline is not allowed to slip.

Other valuable interventions

In addition to the measures set out above, Which? has also identified a number of interventions that may have some value for particular groups of consumers or particular types of fraud. As part of its cost-benefit analysis, the regulator should explore the benefit these measures may deliver, and set out a strong rationale for why it will, or will not, require the industry to adopt them.

Risk warnings at point of transaction

The introduction of generic warning messages at the point of transaction could be effective in some cases of malicious misdirection fraud - for example, where a consumer is already communicating with a third party (such as a solicitor) and a fraudster gains access to the third party's email and then asks the consumer to transfer funds which he or she was already expecting to do.

However, they are unlikely to have much impact on malicious payee fraud, as typically in these types of fraud the victim has 'bought in' to the fraudster's claims and a warning message may be insufficient to override this.

The use of more specific messages when a consumer is attempting to make a payment with concerning characteristics might have more merit, and consumer testing will be important to understand the impact that such an intervention might have on preventing the fraud from taking place.

Repatriation of funds

Where funds can be traced and repatriated they should be, and Which? welcomes measures to improve the tracing and repatriation of funds, as they help to undo the financial harm to consumers from APP fraud. However, we are aware of the challenges to repatriation, notably once funds are transferred abroad, and we believe that these measures will only be effective until the funds leave the banking system, which may be shortly after a fraud is committed.

Alternatives considered

In addition to the approaches outlined above, Which? has considered a number of other interventions, which on balance, we do not think would be appropriate to introduce as blanket solutions.

These include limits on transaction levels, as well as delays in making payments or releasing funds. Our initial view is that these measures would only have a limited impact on malicious payee fraud, and there are better ways to prevent malicious redirection fraud. In addition, any delay in transferring funds could also cause significant cash flow problems for genuine recipients, whether businesses or individuals, which we see as a considerable potential downside.

We recognise that some of these measures may be appropriate in particular circumstances or when applied to specific groups. For example, where a consumer has been identified as vulnerable, or where there is evidence that they have already been a victim of fraud, the bank may choose to raise a flag on their account that would result in a delayed payment or additional measures to be in place for transactions over a certain threshold. However, this would not be appropriate as a blanket approach for the whole of the industry.

Finally, whilst there is value in making consumers more aware of actions they may be able to take to guard against APP fraud, Which? does not believe that education or awareness raising campaigns alone will have a significant impact on reducing the number of people who fall victim to this type of fraud, compared to other interventions the regulator could make. To date, this approach has been industry's primary response to APP fraud, even when informed consumers are not always based placed to identify the risk, and as fraudsters' methods develop and become increasingly sophisticated, any education campaign would need to be constantly renewed (and constantly delivered to reach consumers, who would constantly need to act on this new information).

Vanessa Furey, Senior and International Campaigner Which?, 2 Marylebone Road, London NW1 4DF Vanessa.Furey@which.co.uk020 7770 7325